

ANNEX A

Operations Security

COUNTERINTELLIGENCE

The following table lists procedures and considerations that apply counterintelligence measures are required.

STEP	ACTION – Counterintelligence
1	The sign and countersign are changed daily at the specified time. Challenge unknown personnel at all times and all personnel after dark.
2	PSG personally checks the platoon area prior to departure to ensure no material of intelligence value is left behind.
3	SOI and maps with overlays will be in personal possession of the TC at all times.
4	Crewmen will not keep diaries and will self-censor their outgoing mail.
5	Require authentication of all directives or orders received over the radio from unknown sources.
6	Immediately report the following to the platoon leader: <ul style="list-style-type: none">• Known or suspected compromise of operational material and loss of maps, SOI, ANCD overlays, and other items of tactical value.• Known or suspected enemy agents.• Attempts to subvert unit personnel.

SECURITY READINESS CONDITIONS

REDCON levels allow quick responses to changing situations and ensure completion of necessary work and rest plans. Refer to the chart on page 13 detailing the procedures applicable at each REDCON level.

SIGNAL SECURITY

Levels of signal security are as follows:

- **HUSH-1.** Free net; all FM and digital stations can transmit as necessary.
- **HUSH-2.** Direct net; FM and digital stations are allowed to transmit only when contacted by the platoon leader or higher headquarters.
- **HUSH-3.** Radio listening silence (all stations). No FM traffic; digital transmissions only.
- **HUSH-4.** Radio/digital silence (no traffic of any type).